IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

JOSEPH MAUSTELLER, on behalf of himself and all others similarly situated, Plaintiff, v. LAFAYETTE FEDERAL CREDIT UNION, Defendant.	)	**No.** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Joseph Mausteller, individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Lafayette Federal Credit Union ("LFCU" or "Defendant"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for their failure to exercise reasonable care in securing and safeguarding individuals' sensitive personal data. On September 16, 2024, Defendant LFCU experienced a data breach incident ("Security Breach"). Types of personal data exposed included names, financial account information, loan account number, and Social Security numbers (collectively "Private Information" or "PII").

2. In March of 2025, Plaintiff received a templated notice letter describing the breach of his Private Information.

3. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiff and members of the Class (defined below). These failures put Plaintiff's and Class

members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, emotional grief associated with constant mitigation of personal banking and credit accounts, mitigate and deal with the actual and future consequences of the Security Breach, including, as appropriate, reviewing records for fraudulent charges, reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach.

4. The Security Breach was caused and enabled by Defendant's violation of their obligations to abide by best practices and industry standards concerning the security of consumers' records and Private Information. Defendant failed to comply with security standards and allowed their customers' Private Information to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

5. Accordingly, Plaintiff asserts claims for negligence, breach of implied contract, unjust enrichment/quasi-contract, negligence *per se*, and seeks injunctive relief, monetary damages, and all other relief as authorized in equity or by law.

II. JURISDICTION

6. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

7. The Court has personal jurisdiction over Defendant because Defendant's place of business is located within the District, and Defendant conducts substantial business in this District.

8. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

III. PARTIES

Plaintiff Joseph Mausteller

9. Plaintiff Joseph Mausteller has resided in North Carolina for the time period relevant to this Data Breach.

10. Mr. Mausteller is a current customer of LFCU.

11. Mr. Mausteller provided his Private Information to the Defendant as a condition for receiving banking and financial services. He provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Mr. Mausteller had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

12. Mr. Mausteller has been using LFCU's services since October 2020.

13. In order to obtain financial services from Defendant, Plaintiff was required to provide his Private Information to Defendant.

14. At the time of the Data Breach, LFCU retained Plaintiff Mausteller's Private Information in its system.

15. Plaintiff Mausteller is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

16. Plaintiff Mausteller became aware of the Data Breach through a notice letter dated March 20, 2025, notifying him that his name, financial account number, loan account number and Social Security Number were potentially involved. On the same day he became aware of the Data Breach, Plaintiff immediately took steps to protect and vindicate his rights, including by initiating this litigation.

17. As a result of the Data Breach, Plaintiff Mausteller made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach as well as checking his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

18. Plaintiff Mausteller suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of his Private Information; and (vi) the continued and increased risk of fraud and identity theft.

19. On or around March 4, 2025, Plaintiff Mausteller received a Lafayette Fraud Alert, notifying him of an unauthorized transaction related to Google on his LFCU debit card. Subsequently, Plaintiff had his debit card replaced.

20. Plaintiff Mausteller has suffered an increase in spam and fraudulent messaging since the Data Breach.

21. The Data Breach has caused Plaintiff Mausteller to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify him of the incident.

22. As a result of the Data Breach, Plaintiff Mausteller anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Mausteller is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

23. Plaintiff Mausteller has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant Lafayette Federal Credit Union

24. Defendant Lafayette Federal Credit Union is a company with its principal place of business located in Rockville, Maryland.[1]

25. Defendant LFCU's privacy policy states that it will protect members' privacy and will "use security measures that comply with federal law. These measures include computer

[1] https://www.lfcu.org/contact/ (last accessed March 28, 2025).

safeguards and secured files and buildings. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your non-public personal information..”[2]

IV. FACTS

26. Defendant LFCU operates eight full-service branch locations in Virginia, Maryland, and the District of Columbia.

27. On September 16, 2024, LFCU experienced a data security incident that exposed the Private Information of at least 75,545 individuals. Any other data breaches that may have occurred have not been publicly reported.

28. Defendant LFCU first learned of unusual activity involving an email account whereby an unauthorized party gained access to the records that contained individuals’ Private Information including names, financial information, and Social Security numbers.

29. Defendant has yet to affirmatively notify impacted parties individually regarding which specific pieces of their Private Information were stolen.

30. The Security Breach occurred because Defendant failed to take reasonable measures to protect the Private Information they collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated public warnings to the financial industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on financial institutions. For example, Defendant failed to maintain basic security measures. Defendant failed to disclose to Plaintiff and Class members the material fact that it did not have adequate data security practices to safeguard customers’ personal data, and in fact falsely represented that their security measures were sufficient to protect the Personal Information in their possession.

[2] https://www.lfcu.org/privacy-policy/ (last accessed March 28, 2025).

31. Defendant's failure to provide immediate formal notice of the Breach to Plaintiff and Class members exacerbated the injuries resulting from the Breach.

A. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Consumers' Private Information Despite Previous Data Breaches

32. Defendant was or should have been aware of the risk of data breaches, especially as data breaches in the banking industry are becoming exponentially more common.

33. Defendant failed to ensure that proper data security safeguards were being implemented throughout the breach period.

34. As Defendant acknowledges, Defendant had obligations created by industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Plaintiff and Class members provided their Private Information to LFCU with the reasonable expectation and mutual understanding that LFCU and any of its affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

36. Prior to and during the Security Breach, LFCU promised clients that their Private Information would be kept confidential unless for the reasons listed in their Privacy Policy or Plaintiff so authorized. Hackers taking Plaintiff's information was not included.

37. Defendant's failure to provide adequate security measures to safeguard clients' Private Information is especially egregious because Defendant operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to individuals' highly confidential Private Information.

38. Defendant has been on notice for years that the financial industry is a prime target for scammers because of the amount of confidential client information maintained. Recently, a

number of high-profile data breaches have rocked the financial and banking industries. For instance, major high-profile data breaches have impacted this industry, including the Equifax and Capital One data breaches.

B. Damages to Plaintiff and the Class

39. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Security Breach.

40. Plaintiff and the Class have experienced or currently face a substantial risk of out-of-pocket fraud losses such as, *e.g.*, loss of funds from bank accounts, fraudulent charges on credit cards, targeted advertising, suspicious phones calls, and similar identity theft.

41. Class members have or may also incur out of pocket costs for protective measures such as credit freezing or payment for phone scam detection,

42. Plaintiff and Class members suffered a "loss of value" of their Private Information when it was acquired by cyber thieves in the Security Breach. Numerous courts have recognized the propriety of "loss of value" damages in data breach cases.

43. Class members who paid Defendant for services, or who contracted with other companies that paid Defendant, were also damaged via "benefit of the bargain" damages. Such members of the Class overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price paid to Defendant was intended to be used by Defendant to fund adequate data security. Defendant did not properly comply with their data security obligations. Thus, the Class members did not get what they were owed.

44. Members of the Class have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

45. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[3]

46. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[4]

47. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit and tax filings for an indefinite duration.

C. The Value of Privacy Protections and Private Information

48. The fact that Plaintiff's and Class members' Private Information was stolen—and might presently be offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

[3] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://bjs.ojp.gov/content/pub/pdf/vit14.pdf

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id.*

49. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[5]

50. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[6]

51. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[7]

---

[5] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001) available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf

[6] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274

[7] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

52. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[8] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

53. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[9]

54. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the financial industry.

55. Had Defendant followed industry guidelines and adopted security measures recommended by experts in the field, Defendant would have prevented intrusion into their systems and, ultimately, the theft of their clients' Private Information.

56. Given these facts, any company that transacts business with individuals or on their behalf and then compromises the privacy of clients' Private Information has thus deprived clients of the full monetary value they are entitled to.

---

[8] *Web's Hot New Commodity: Privacy*, *supra* note 7.

[9] *See* DOJ, *Victims of Identity Theft, 2014*, *supra* note 3, at 6.

57. Due to damage from Defendant, Plaintiff and the other Class members now face a greater risk of continuous identity theft.

D. CLASS ACTION ALLEGATIONS

58. Plaintiff brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Nationwide Class defined as:

> All persons who had their private information compromised and received a notice letter from Defendant as a result of the Data Breach occurring on or around September 16, 2024, (the "Nationwide Class").

59. Excluded from both the Nationwide Class and are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

60. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

61. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the tens of thousands.

62. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

63. Whether Defendant's data security systems prior to and during the Security Breach complied with applicable data security laws and regulations including, *e.g.,* FTC Act;

64. Whether Defendant's data security systems prior to and during the Security Breach were consistent with industry standards;

65. Whether Defendant properly implemented their purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

66. Whether Defendant took reasonable measures to determine the extent of the Security Breach after they first learned of same;

67. Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

68. Whether Defendant's conduct constitutes breach of an implied contract;

69. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff' and the Class's Private Information;

70. Whether Defendant was negligent in failing to properly secure and protect Plaintiff' and the Class's Private Information;

71. Whether Defendant was unjustly enriched by their actions; and

72. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

73. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other members of the Class. Similar

or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

74. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

75. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because his interests do not conflict with the interests of the Classes he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

76. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

77. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the

Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

V. CAUSES OF ACTION

COUNT I
Negligence

78. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

79. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

80. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

81. Defendant owed numerous duties to Plaintiff and the Class, including the following:

a) to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

b) to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c) to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

82. Defendant also breached its duty to Plaintiff and the Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

83. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the financial industry.

84. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff' and Class members' Private Information.

85. Defendant breached their duties to Plaintiff and the Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

86. Because Defendant knew that a breach of their systems would damage thousands of their customers, including Plaintiff and the Class members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

87. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and their clients, which is recognized by

laws and regulations including but not limited to common law. Defendant was in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

88. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

89. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

90. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and the Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

91. Defendant breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Security Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

e. Failing to timely notify Class members about the Security Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

92. Through Defendant's acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or control.

93. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

94. Neither Plaintiff nor the other Class members contributed to the Security Breach and subsequent misuse of their Private Information as described in this Complaint.

95. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

96. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
Breach of Implied Contract

97. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

98. Defendant solicited and invited Class members or others other entities working on their behalf to provide their Private Information as part of Defendant's regular business practices. When Plaintiff and Class members or other entities operating on their behalf made and paid for purchases of Defendant's services and products, they provided their Private Information to Defendant.

99. In so doing, Plaintiff and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

100. Class members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

101. Plaintiff and Class members would not have provided and entrusted their Private Information with Defendant in the absence of the implied contract between them and Defendant.

102. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

103. Defendant breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the data breach within a reasonable time.

104. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant, Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

105. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class members.

COUNT III
Unjust Enrichment/Quasi-Contract

106. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

107. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they or other entities operating on their behalf purchased goods and services from Defendant and provided Defendant with their Private Information. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

108. Defendant knew that Plaintiff and Class members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendant profited from this and used Plaintiff's and the Class members' Private Information for business purposes.

109. Defendant failed to secure Plaintiff's and the Class members' Private Information and, therefore, did not provide full compensation for the benefit of the Plaintiff's and Class members' Private Information provided.

110. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

111. If Plaintiff and the Class members knew that Defendant would not secure their Private Information using adequate security, they would not have allowed entities to entrust Defendant with their Personal Information.

112. Plaintiff and Class members have no adequate remedy at law.

113. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

114. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT IV
Negligence Per Se

115. Plaintiff restates and re-alleges all preceding paragraphs as if fully set forth herein.

116. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' PII.

117. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and Class members' sensitive Private Information. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Trionfo, of failing to use reasonable measures to protect clients' PII.

118. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its clients' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII LFCU had collected and stored and the foreseeable consequences of a data breach, including the immense damages that would result to its clients in the event of a breach, which ultimately came to pass.

119. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

120. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard their PII.

121. Defendant breached their duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' PII.

122. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

123. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

124. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

125. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have

known that it was failing to meet its duties and that its breach would cause Plaintiff and the Class to suffer the foreseeable harms associated with the exposure of their PII.

126. Had Plaintiff and members of the Class known that Defendant did not adequately protect the PII entrusted to it, Plaintiff and members of the Class would not have entrusted LFCU with their PII.

127. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including, but not limited to, loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the treatment Plaintiff and members of the Class paid for that they would not have sought had they known of Defendant's careless approach to cyber security; lost control over the use of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Nationwide Class as requested herein, designating Plaintiff as Nationwide Class Representatives, and appointing Class Counsel as requested in Plaintiff' expected motion for class certification;

B. Ordering Defendant to pay actual damages to Plaintiff and the other members of the Class;

C. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

D. Ordering injunctive relief requiring Defendant to, *e.g.*: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members;

E. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and his counsel;

F. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

G. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

H. Ordering such other and further relief as may be just and proper.

Date: March 28, 2025

Respectfully submitted,

By: /s/ *Jason S. Rathod*
Jason S. Rathod
jrathod@classlawdc.com
Nicholas A. Migliaccio
nmigliaccio@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

Counsel for Plaintiff